LISTING OF THE CLAIMS

1-42. (cancelled)

43. (new) A method of performing graded user authentication over a network, the method comprising:

obtaining first circumstantial data during a first authentication attempt by a first user;

storing said first circumstantial data;

obtaining second circumstantial data during a second authentication attempt by a second user;

obtaining authorization data during said second authentication attempt by said second user;

comparing said second circumstantial data to said stored first circumstantial data; and

assigning a level of trust to said second user.

44. (new) The method of claim 43, wherein said first user attempts said first authorization from a first location and said second user attempts said second authorization from a second location which is separate and distinct from said first location.

45. (new) The method of claim 43, wherein said first user and said second user are the same user.

46. (new) The method of claim 43, wherein said first authentication attempt is successful.

47. (new) The method of claim 44, wherein a session is created after said successful first authentication attempt and said session is closed prior to said second authentication attempt.

48. (new) The method of claim 43, wherein said circumstantial data is data describing one or more aspects of the current circumstances surrounding the authentication attempt with which it is associated.

49. (new) The method of claim 48, wherein said circumstantial data is data describing one or more aspects of the current circumstances surrounding the system of the user seeking to be authorized.

50. (new) The method of claim 49, wherein said circumstantial data comprises an identification associated with said system.

51. (new) The method of claim 50, wherein the identification comprises a processor serial number.

52. (new) The method of claim 49, wherein the circumstantial data comprises an identification associated with the network location of said system.

53. (new) The method of claim 52, wherein the identification comprises an IP address.

54. (new) The method of claim 48, wherein the circumstantial data comprises a time stamp associated with the time at which the authorization was attempted.

55. (new) The method of claim 49, wherein the circumstantial data comprises an identifier associated with the type of network to which said system is connected.

56. (new) The method of claim 43, wherein assigning a level of trust to said second user comprises examining the results of said comparison of said second circumstantial data to said stored first circumstantial data.

57. (new) The method of claim 43, wherein said authorization data is generated using one or more of one or more authorization techniques.

58. (new) The method of claim 57, wherein one of said one or more authorization techniques comprises fingerprint analysis.

59. (new) The method of claim 57, wherein one of said one or more authorization techniques comprises password comparison.

60. (new) The method of claim 57, wherein one of said one or more authorization techniques comprises smart card identification.

61. (new) The method of claim 57, wherein each of said one or more authorization techniques is assigned a reliability index based upon the inherent reliability of that technique.

62. (new) The method of claim 61, wherein assigning a level of trust to said second user comprises examining the reliability indexes of the one or more authentication techniques used to generate said authentication data.

63. (new) A system for graded user authentication over a network comprising:

first circumstantial data obtained during a first authentication attempt by a first user;

second circumstantial data obtained during a second authentication attempt by a second user;

authorization data obtained during said second authentication attempt by said second user; and

a trust engine which assigns a level of trust to said second user.

64. (new) The system of claim 63, wherein said first user attempts said first authorization from a first location and said second user attempts said second authorization from a second location which is separate and distinct from said first location.

65. (new) The system of claim 63, wherein said first user and said second user are the same user.

66. (new) The system of claim 63, wherein said first authentication attempt is successful.

67. (new) The system of claim 63, wherein a session is created after said successful first authentication attempt and said session is closed prior to said second authentication attempt.

68. (new) The system of claim 63, wherein said circumstantial data is data describing one or more aspects of the current circumstances surrounding the authentication attempt with which it is associated.

69. (new) The system of claim 68, wherein said circumstantial data is data describing one or more aspects of the current circumstances surrounding the system of the user seeking to be authorized.

70. (new) The system of claim 69, wherein said circumstantial data comprises an identification associated with said system.

71. (new) The system of claim 70, wherein the identification comprises a processor serial number.

72. (new) The system of claim 69, wherein the circumstantial data comprises an identification associated with the network location of said system.

73. (new) The system of claim 72, wherein the identification comprises an IP address.

74. (new) The system of claim 68, wherein the circumstantial data comprises a time stamp associated with the time at which the authorization was attempted.

75. (new) The system of claim 69, wherein the circumstantial data comprises an identifier associated with the type of network to which said system is connected.

76. (new) The system of claim 63, wherein assigning a level of trust to said second user comprises examining the results of said comparison of said second circumstantial data to said stored first circumstantial data.

77. (new) The system of claim 63, wherein said authorization data is generated using one or more of one or more authorization techniques.

78. (new) The system of claim 77, wherein one of said one or more authorization techniques comprises fingerprint analysis.

79. (new) The system of claim 77, wherein one of said one or more authorization techniques comprises password comparison.

80. (new) The system of claim 77, wherein one of said one or more authorization techniques comprises smart card identification.

81. (new) The system of claim 77, wherein each of said one or more authorization techniques is assigned a reliability index based upon the inherent reliability of that technique.

82. (new) The system of claim 81, wherein assigning a level of trust to said second user comprises examining the reliability indexes of the one or more authentication techniques used to generate said authentication data.